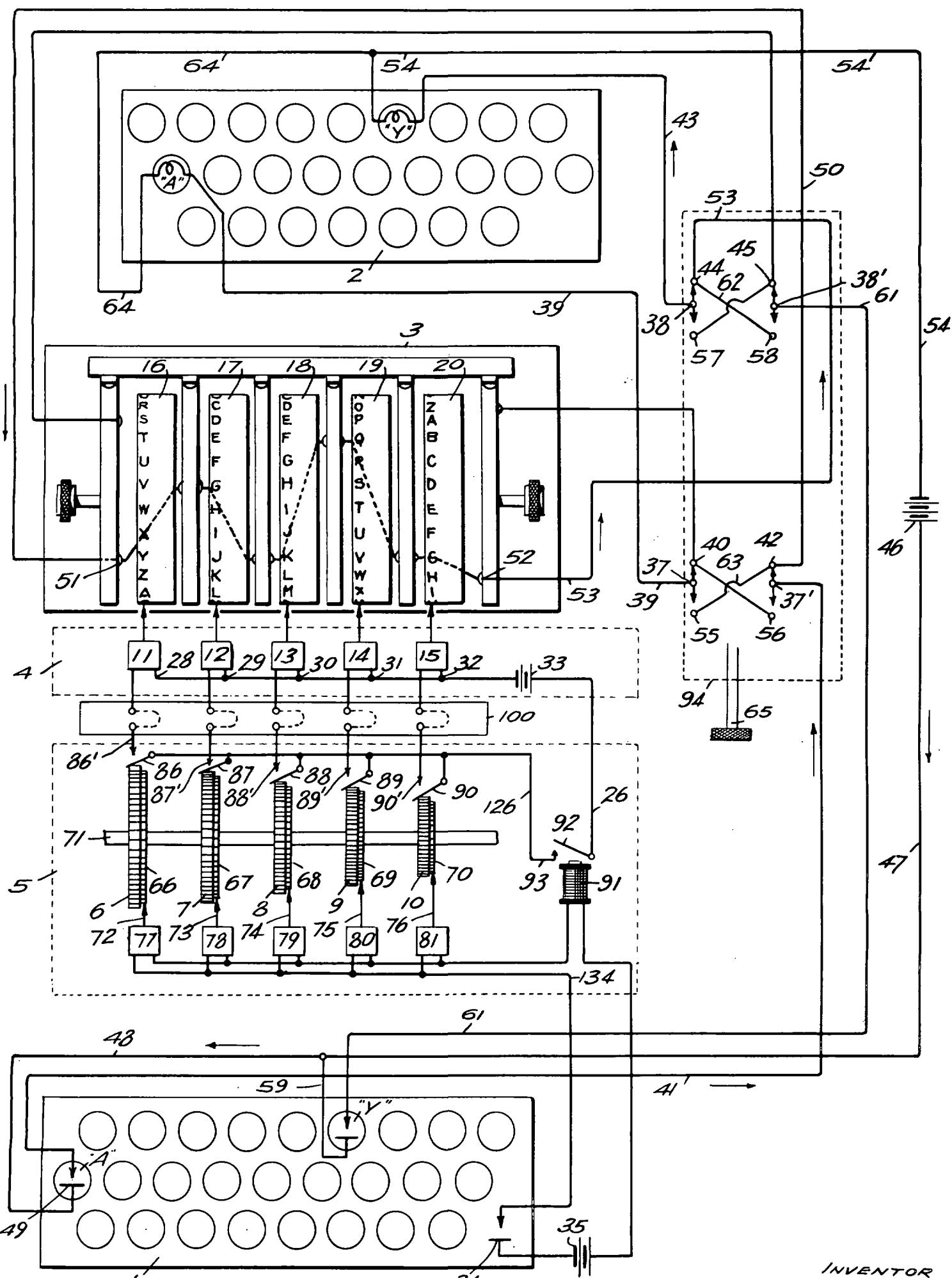


~~Confidential~~P file
Mod. 134-T2

FIG. 1.

INVENTOR
WILLIAM F. FRIEDMAN

Ruth Haughlin

BY and Charles Q. Rose

Confidential

FIG. 2.

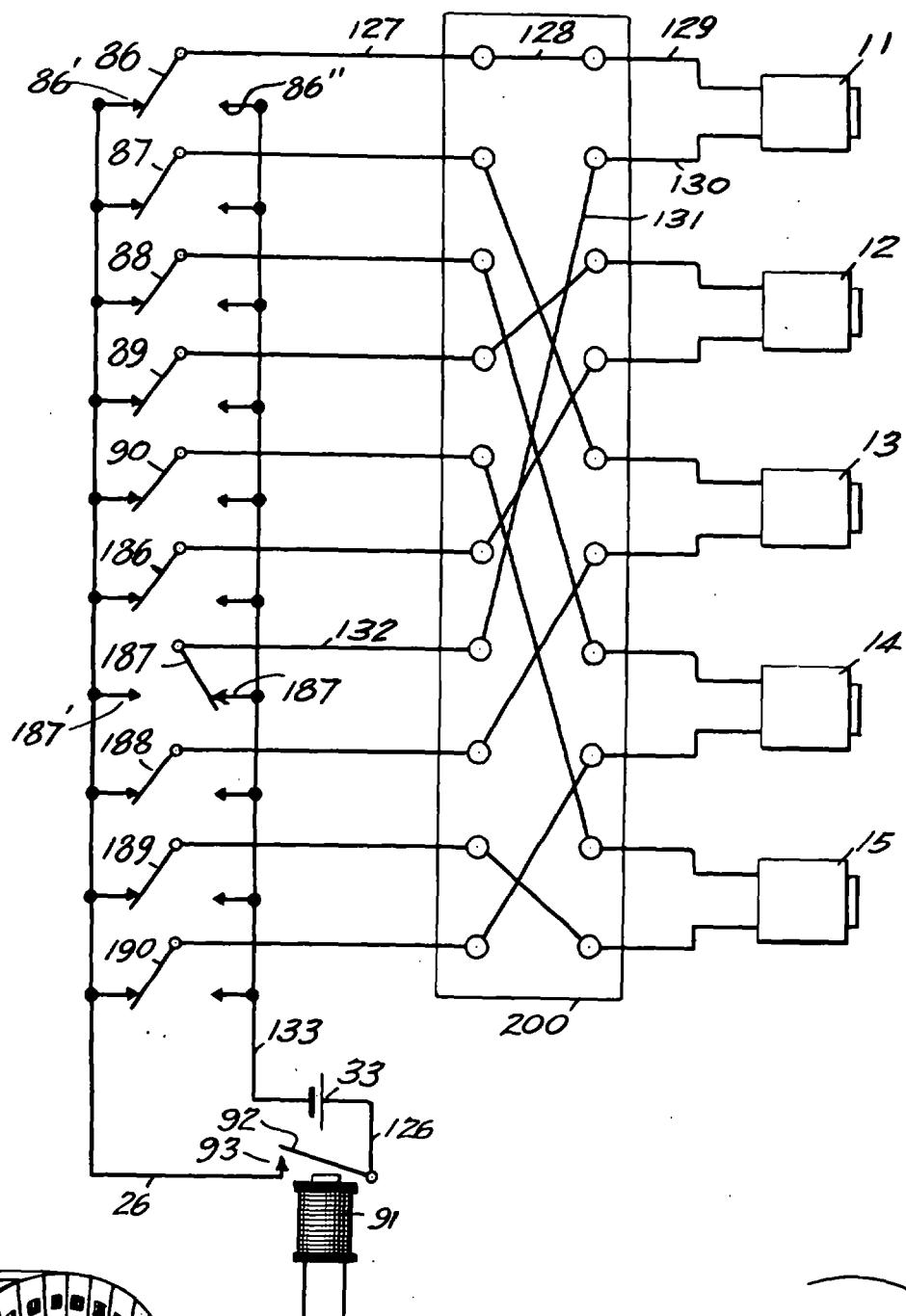
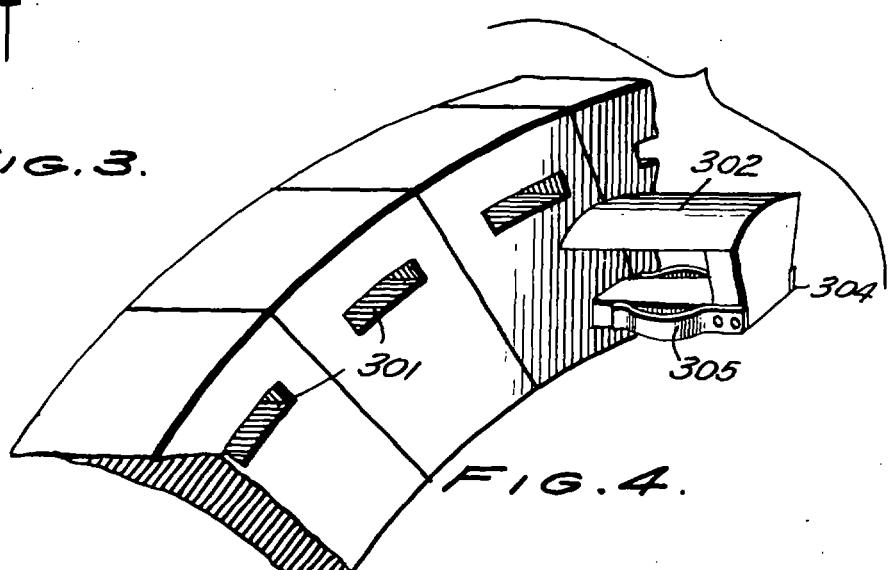
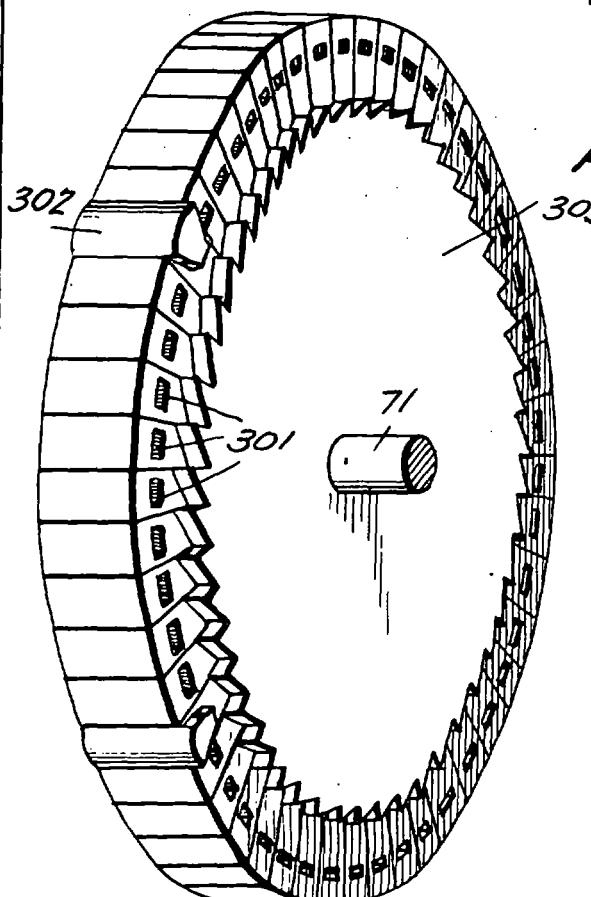


FIG. 3.



INVENTOR
WILLIAM F. FRIEDMAN
By
Ruth Hauglin and
Charles A. Rowe

ATTORNEYS

~~Confidential~~Rec'd 7/26 107, 24-6
File Oct. 22 - 1936

This invention relates to cryptographs and is an improvement based upon the subject-matter of my prior application Serial No. 682,096, filed July 25, 1933.

In said application Serial No. 682,096, I disclose a cryptographic system and mechanism, the basic feature of which is the provision of means for aperiodically controlling a set of juxtaposed switching or cipher commutators giving cryptographically a cascade effect. In that system the means referred to involves the use of a cipher-key transmitter through which a perforated key-tape is passed.

The object of this invention is to control the juxtaposed cipher commutators by means of an associated set of cam wheels of different diameters, thus dispensing with the perforated tape referred to above.

The invention is illustrated in the accompanying drawings, in which :

Fig. 1 is a schematic diagram of the mechanism, including a set of five cam wheels controlling a corresponding number of electro-magnetic, stepping devices for effecting angular displacement of the commutators;

Fig. 2 shows paired circuits corresponding to a set of ten cam wheels for electrically controlling the five electro-magnetic, stepping devices of Fig. 1, together with switching means for interchanging the electrical conditions set up by the cam wheels;

Fig. 3 shows a detail of one of the cam wheels ; and
Fig. 4 is another detail showing a replaceable cam element and
mode of assembly with the wheel.

Referring to Fig. 1, there are shown the following elements which are well-known in the art applicable to modern cryptographs employing rotatable cipher commutators: The numeral 1 generally designates a standard typewriter keyboard provided with a set of keys for closing a set of contacts corresponding to character elements; the numeral 2 generally designates a bank of recording or indicating devices which may take the form of a set of magnets of a printing mechanism, or a set of glow lamps to indicate by illumination of superimposed lettering the character equivalents resulting from operation of the keyboard; the numeral 3 generally designates a set of juxtaposed, rotatable circuit changers constructed in the form of switching commutators commonly called cipher commutators, mountable upon a common shaft and arranged to rotate relative to one another and to fixed end plates, in order to provide a large number of variable paths for the passage of an electric current representing a message character set up on the keyboard, the exact path traversed in each instance being determined by the relative rotatory positions of the whole set of cipher commutators and end plates at that instant ; numeral 4 generally designates a set of stepping mechanisms for effecting angular displacements of the cipher commutators. The essence of the present invention consists in the provision of means,

indicated generally at 5, for controlling these stepping mechanisms through the intermediary of a set of pawls and ratchets, and cam wheels associated with the ratchets, the cams opening and closing circuits for operating the electro-magnetically controlled stepping mechanisms.

The most important elements of the cipher commutator control assembly 5, are as follows: A set of five cam wheels 6, 7, 8, 9, and 10, are mounted upon a common shaft 71 upon which they are individually free to rotate. Rigidly fixed to each cam wheel are the respective ratchets 66, 67, 68, 69, and 70, driven by pawls 72, 73, 74, 75, and 76 under the action of magnets 77, 78, 79, 80, and 81. These magnets are actuated by a set of circuits having a common conductor 134, in which is inserted universal keyboard contact 34. Each ratchet has a different number of teeth, the numbers preferably being prime to one another. For example, let ratchets 66, 67, 68, 69, and 70 have 51, 50, 49, 47, and 43 teeth, respectively. The cam wheels associated with the various ratchets are of varying diameters and have their peripheries divided up into numbers of segments corresponding with the numbers of teeth on the ratchet to which each cam wheel is attached; so that, for example, cam wheel 6 has its periphery divided up into 51 equal segments, cam wheel 7 has its periphery divided up into 50 equal segments, and so on. The segments on the various cam wheels are made of equal angular length and, for keying purposes, they are numbered so that the set of cam wheels can be aligned to a bench mark according to a prearranged key. The segments of each cam wheel are slotted out at 301, and into these slots are inserted small slideable plates. These plates are formed with curved or

arcuate upper surfaces, so that when inserted in the slots these curved surfaces project above the rim of the wheel and function as cams. It will be understood that the other segments have their surfaces coincident or flush with the perimeter or outer rim surface of the cam wheel. The distribution of the said cam plates which are to be inserted in each cam wheel in relation to the other segmental surfaces constitutes one of the elements of the cipher key to the system. These plates together with the remaining segmental elements of the wheels control contact levers 86, 87, 88, 89, and 90 and their respective contacts 86', 87', 88', 89' and 90'; that is, when a plate with a cam surface is presented to contact lever 86, for example, the cam action serves to close contact 86', otherwise that contact remains open. Contact levers 86, 87, 88, 89, and 90 control stepping magnets 11, 12, 13, 14, and 15, which operate the stepping mechanisms of the cipher commutators, in a manner presently to be explained.

With the arrangement of cam wheels shown in Fig. 1, the cryptographic period of the assembly of cipher commutators is equal to the product of the numbers of teeth in the set of ratchets 66, 67, 68, 69, and 70. In this case, with the numbers of teeth being 51, 50, 49, 47, and 43 respectively, the period is 252,523,950.

The manner in which the system as a whole functions will now be described. The first step, of course, is to set the cryptograph to the predetermined key. This comprises the following elements: the horizontal permutation or arrangement of cipher commutators on the shaft; the rotatory alignment of the commutators, according to a group of letters aligned on a bench mark; the exact distribution of the slideable plates

in their relation to the other segmental elements of the cam wheels; the rotatory alignment of the cam wheels according to a group of characters aligned on a bench mark; finally, the cryptograph is set to the enciphering position. When the key corresponding to "A" is depressed on the keyboard a current flows from battery 46, along conductors 47, 48, to closed contact 49, conductor 41, contacts 57, 48, conductor 50, contacts 51 on the left end plate of the cipher commutators, thence through the commutators, emerging at contact 52 on the right end plate, conductor 53, contacts 44, 38, conductor 43, to lamp or indicating device "Y", conductor 54 back to battery 46. Upon release of key "A", and at the end of the return excursion or back stroke of a universal bar on the keyboard, universal contact 84 is closed and a circuit is passed through the set of magnets 77, 78, 79, 80, and 81, causing the pawls 72, 73, 74, 75, and 76 to act so that cam wheels 6, 7, 8, 9, and 10 are advanced one step. A single magnet can of course be used for this purpose, with mechanical means of affecting each pawl. The universal keyboard contact circuit includes relay 91 which controls contact lever 92 and contact 93, which is in the circuit controlling magnets 11, 12, 13, 14, and 15, so that current can pass through the latter magnets only at the instant when the universal contact is closed. When the cam wheels 6, 7, 8, 9, and 10 are advanced one step, a new combination of operative and inoperative contact levers 86 to 90 and of open and closed contacts 86', 87', 88', 89', and 90' is set up, and corresponding thereto magnets 11, 12, 13, 14, and 15 are actuated.

These control the displacement mechanisms associated with the cipher commutators and set up a new path through the commutators for the encipherment of the next letter.

To decipher the message, screw 65 is revolved to set the switch plate 94 to the deciphering position. The cipher commutators and the cam wheels must of course also be returned to their initial position and arrangement in enciphering. It is unnecessary to trace the deciphering circuits through, since this phase of operation by means of a reversing switch is well known in the art.

It would be easy to provide means, consisting of a simple switchboard 100 with a plug and jack arrangement for connecting contacts 86' to 90' to magnets 11 to 15 in any one of 120 different permutations.

In FIG. 1 I have shown an assembly of but five cam wheels, one for each cipher commutator. But it is readily possible to have a set of ten cam wheels which can be electrically combined into five pairs to control the five cipher commutators. This is shown schematically in FIG. 2, in which 11, 12, 13, 14, and 15 are the similarly numbered magnets of FIG. 1, for controlling the stepping mechanisms of the cipher commutators. Contact lever 86 is the same as the similarly numbered contact lever of FIG. 1, except that this lever is now associated with two contacts, a lower contact 86', against which it normally rests, and an upper contact 86" which it touches when a button on the cam wheel is presented to the contact lever 86. Contact levers 87, 88, 89, and 90 are of the same form

as contact lever 86, and serve similar functions; they are homologous to similarly numbered levers of Fig. 1 and, like contact lever 86 of Fig. 2, they are each associated with paired contacts. Contact levers 186, 187, 188, 189, and 190 are five additional contact levers similar to 86, 87, 88, 89, and 90; they are associated with and operated by five additional cam wheels, so that there are now ten cam wheels and ten contact levers. If the numbers of segments on cam wheels 6, 7, 8, 9, and 10 of Fig. 1, are as indicated before, namely, 51, 50, 49, 47, and 43, the numbers of segments on the additional five cam wheels may, for example, be 41, 37, 31, 29, and 23. The complete period of the whole system of cam wheels in this case would be $51 \times 50 \times 49 \times 47 \times 43 \times 41 \times 37 \times 31 \times 29 \times 23$.

In Fig. 2, the switchboard 200 serves as a means for interconnecting the contact levers 86, 87, 88, 89, 90, 186, 187, 188, 189, and 190 in pairs, and by a multitude of different arrangements, so that the five sets of paired contact levers control the five magnets 11, 12, 13, 14, and 15 by a paired relationship explained below. For example, as interconnected in Fig. 2, magnet 11 is controlled jointly by contact levers 86 and 187; magnet 12 is controlled jointly by contact levers 188 and 189; magnet 13, by 90 and 186; magnet 14, by 88 and 190; magnet 15, by 87 and 89. The relay 91 in Fig. 2 is the same as the similarly numbered relay in Fig. 1 and serves the same function, namely, to apply potential to the circuits controlled by contact levers 86, 87, 88, 89, 90, 186, 187, 188, 189, 190 only on the back stroke of the universal bar on the keyboard.

The manner in which a magnet 11 of Fig. 2, for example, is controlled by its temporarily associated contact levers, in this case 86 and 187, is as follows: Suppose contact lever 86 is at its lower position, against contact 86', there being at that moment on the periphery of the first cam wheel a segment which is flush with the rim of the wheel, that is, no cam surface is presented to contact lever 86; that at the same moment contact lever 187 is at its upper position, against its upper contact 187', there being at that moment on the periphery of the seventh cam wheel a plate which bears a projecting cam surface. A circuit is established thus: battery 33, conductor 186, contact lever 86 of relay 91, which is at that moment energized from the keyboard as explained above, contact 93, conductor 26, contact 86', contact lever 86, conductor 187, flexible conductor 128 of switchboard 200, conductor 129, through magnet 11, conductor 130, flexible conductor 131 of switchboard 200, conductor 132, contact 187" against which contact lever 187 is now resting, conductor 133, back to battery 33. Magnet 11 is energized. It will be seen that magnet 11 is subject to four conditions:

- (1) Contact lever 86 is making contact at 86' when contact lever 187 is making contact at 187". No circuit will be established through magnet 11, because both levers are then connected to the same side of the battery 33.
- (2) Contact lever 86 is making contact at 86' when contact lever 187 is making contact at 187". A circuit will be established through magnet 11.

(3) Contact lever 86 is making contact at 86' when contact lever 187 is making contact at 187'. A circuit will be established through magnet 11.

(4) Contact lever 86 is making contact at 86" when contact lever 187 is making contact at 187". No circuit is established through magnet 11.

The same set of four conditions applies to magnets 12, 13, 14, and 15 and their associated contact levers and contacts.

By interchanging the connections established at switchboard 200 great variability in electrical effects of the set of contact levers is afforded for cryptographic keying purposes.

In Fig. 3 is shown a detail of one of the cam wheels, with its slots 301, removable plates 302, and ratchet 303. The removable plates 302 are provided with springs 304, 305 to hold the plate in place when inserted in the slot.

Changes, modifications and equivalent arrangements are contemplated within the scope of the invention as defined by the appended claims:

I claim :

1. In a cryptograph, a keyboard comprising character elements and corresponding signaling elements in operative electrical connection therewith ; means comprising a set of juxtaposed, rotatable commutators for varying the connections between the keyboard elements and said signaling elements ; a set of cam-bearing rotatable members; means for angularly-displacing said members upon operation of said keyboard; a set of contact layers and associated contacts controlled by said cam-bearing members; and means coordinated with said set of cam-bearing members to effect permutative, step-wise displacements of the commutators.

2. In a cryptograph, a keyboard comprising character elements and corresponding signaling elements in operative electrical connection therewith ; means comprising a set of juxtaposed, rotatable commutators for varying the connections between the keyboard elements and said signaling elements ; a set of cam-bearing members; means for angularly displacing said members upon operation of said keyboard; and means coordinating said cam-bearing members with the commutators to effect permutative, stepwise displacements of the commutators.

3. In a cryptograph, a keyboard comprising character elements and corresponding signaling elements electrically interrelated therewith ; means comprising a set of juxtaposed, rotatable commutators

for varying the relationship between the keyboard elements and said signaling elements ; a set of cam-bearing rotatable members; means for angularly displacing said members upon operation of said keyboard; and a series of commutator stepping mechanisms, the cam-bearing members being [electrically] associated with the commutator stepping mechanisms to effect permutative, stepwise displacements of the commutators.

4. In a cryptograph, a keyboard comprising character elements and corresponding signaling elements electrically interconnected therewith ; means comprising a set of juxtaposed, rotatable commutators for varying the connections between the keyboard elements and said signaling elements ; a plurality of sets of cam-bearing rotatable members ; means for effecting stepwise angular displacements of said cam-bearing members with individual depressions of the keys of said keyboard; and means coordinating said sets of cam-bearing members to effect permutative, stepwise displacements of the commutators.

5. In a cryptograph, a keyboard comprising character elements and corresponding signaling elements electrically interconnected therewith ; means comprising a set of juxtaposed, rotatable commutators for varying the connections between the keyboard elements and said signaling elements ; a plurality of cam-bearing members; means for effecting stepwise angular displacements of said cam-bearing members with individual key operation of said keyboards; a series of commutator stepping mechanisms each comprising an electro-magnet and an associated ratchet

and pawl, each ratchet and pawl actuating its associated commutator, the set of commutator stepping mechanisms being controlled by the said cam-bearing members associated as a group and coordinated collectively to effect permutative, stepwise displacements of the commutators.

6. A mechanism of the character described in claim 5 in which the periphery of each cam-bearing member is divided up into equal-spaced segments, the numbers of segments on the respective cam-bearing members being prime to one another.

7. In a cryptograph, a keyboard comprising character elements and corresponding signaling elements electrically interconnected therewith; means comprising a set of juxtaposed, rotatable commutators for varying the connections between the keyboard elements and said signaling elements; a set of commutator stepping mechanisms corresponding in number to the number of said commutators; a set of contact levers and associated contacts controlling the operation of said commutator stepping mechanisms; rotatable cam-bearing members for operating said contact levers; and means for angularly displacing said cam-bearing members upon successive depressions of the keys of said keyboard.

8. A mechanism of the character described in claim 7 in which the numbers of [cams] on the respective cam-bearing members are prime to one another.

9. In a cryptograph of the character described, the combination of [electrically] related keyboard elements and signaling elements; a set

of juxtaposed, rotatable commutators for varying the relationships between the two sets of elements ; a series of commutator stepping mechanisms for displacing the respective commutators in a stepwise manner ; a set of cam-bearing members for controlling the commutator stepping mechanisms to effect the stepwise displacements of the commutators in a permutative manner ; and means for effecting stepwise displacements of said cam-bearing members.

24 Aug 57
 10. In a cryptograph of the character described, the combination of electrically interrelated keyboard elements and signaling elements ; a set of juxtaposed rotatable commutators for varying the relationship between the two sets of elements ; a set of commutator stepping mechanisms for displacing the respective commutators in a stepwise manner ; and a plurality of rotatable cam-bearing members for collectively controlling the commutator stepping mechanisms to effect the stepwise displacements of the commutators in a permutative manner. [and aperiodic] Substantially

11. A mechanism of the character described, comprising a set of elements constituting a keyboard, and a set of elements constituting a signaling bank, said sets of elements being electrically interrelated ; a set of juxtaposed, rotatable switching devices for varying the electrical relation between the two sets of elements ; and means for effecting stepwise displacements of the switching devices in an irregular manner, said means including a set of rotatable cam-bearing members controlling the stepwise displacements of the switching devices.

24 Aug 37

12. In combination a set of character elements constituting a keyboard; a switch individual to each element and operable thereby; a corresponding number of translating devices operable by said elements; a wiring system interposed between said switches and said translating devices rendering available a multiplicity of electrical paths between said switches and said devices; and means acting in response to each key operation for selecting a group of said paths, said last named means comprising a set of contact levers and associated contacts, and a plurality of rotatable cam-bearing members angularly displaceable in response to each key operation for controlling said levers and contacts, the numbers of [cams] on the respective cam-bearing members being prime to one another.

13. In combination a set of character elements constituting a keyboard; a switch individual to each element and operable thereby; a corresponding number of translating devices operable by said elements; a wiring system interposed between said switches and said translating devices rendering available a multiplicity of electrical paths between said switches and said devices whereby each switch may become associated with any one of a plurality of said translating devices, said system comprising adjustably movable connectors whereby the wiring system may be given an initial setting providing one electrical path for each switch; and means operable in respect to each key operation for changing such setting, said last-named means comprising a set of cam-bearing members angularly displaceable in response to individual key operation, a set of contact levers and associated contacts operated by said cam-bearing members, said contact levers and contacts controlling the association of each said switch with any one of said plurality of translating devices.

15